

## Logging & Reporting: New Features & Changes

- NAC Quarantine simplification
- Captive Portal
- HTTP header replacement for Virtual Servers
- IPv6
- TCP Reset when session automatically closed
- CoS Support

## NAC Quarantine simplification

- Many quarantine options have been removed. They will be added back in Future firmware versions.
- DLP sensor: only option is quarantine-ip to quarantine all traffic from the IP address.
- Antivirus profile: only option is quar-src-ip to quarantine all traffic from the source IP.
- IPS sensor: only option is block attacker's IP.
- IPv4 & IPv6 DoS-policies: only option is attacker to block attacker's IP.

3

FORTINET

## Captive Portal

- In 5.0, Captive portal was a mechanism for capturing authentication through the wireless
- In 5.2, Captive portal is used for capturing user authentication on an interface (wireless or otherwise)

4

FORTINET

## HTTP header replacement for Virtual Servers

- By default, if `http-ip-header` is enabled in a virtual-server configuration then as HTTP(S) traffic flows through a virtual server FortiOS either adds an *X-Forward-For* header with the client's original IP address or updates any existing *X-Forwarded-For* header with the client's IP address. Some servers want the client's original IP address, but do not want to use *X-Forwarded-For* and instead want a configurable name to be used. The new attribute `http-ip-header-name` allows this name to be defined.
  - » If defined, then any existing *X-Forwarded-For* header is removed.

5

FORTINET

## HTTP header replacement for Virtual Servers: CLI Config

```
config firewall vip
    edit (vip name)
        set type server-load-balance
        set server-type https
        Set http-multiplex enable
        set http-ip-header enable
        set http-ip-header-name <name of header to add>
    end
```

- `server-type` of `http` and `http-multiplex enable` are required settings to be use this functionality.

6

FORTINET

## IPv6: TCP Clamping

- 5.0.x (and previous) and TCP Clamping for IPv4 (CLI Only, per policy)

```
config firewall policy
    edit (policy id)
        set tcp-mss-sender [MSS value to set on egress traffic]
        set tcp-mss-receiver [MSS value to set on ingress traffic]
    end
```

- 5.2 adds support in IPv6 policies

- » IPv6
- » NAT66
- » NAT46/NAT64

7

FORTINET

## IPv6: TCP Clamping (Wireshark)

```
FortiGate-VM64 (1) # sh
config firewall policy6
    edit 1
        set uuid 87b4d704-9b1c-51e3-3772-ef3239e6a244
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set tcp-mss-sender 1200
        set tcp-mss-receiver 1000
    next
end
```

No.	Time	Source	Destination	Protocol	Length	Info
3	2005-01-01 00:00:01.419727	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	49244 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=4 SACK_PERM=1
4	2005-01-01 00:00:01.419769	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	49244 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1200 WS=4 SACK_PERM=1
5	2005-01-01 00:00:01.420079	2142::2038:1a37:e72f:1885	2040::60f1:52e4:af04:72da	TCP	86	ftp > 49244 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=4 SACK_PERM=1
6	2005-01-01 00:00:01.420096	2142::2038:1a37:e72f:1885	2040::60f1:52e4:af04:72da	TCP	86	ftp > 49244 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1000 WS=4 SACK_PERM=1
7	2005-01-01 00:00:01.420148	2142::2038:1a37:e72f:1885	2040::60f1:52e4:af04:72da	TCP	86	ftp > 49244 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=4 SACK_PERM=1
8	2005-01-01 00:00:01.420155	2142::2038:1a37:e72f:1885	2040::60f1:52e4:af04:72da	TCP	86	ftp > 49244 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1000 WS=4 SACK_PERM=1
9	2005-01-01 00:00:01.420691	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0 SRE=0
10	2005-01-01 00:00:01.420699	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#1] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
11	2005-01-01 00:00:01.420736	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#2] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
12	2005-01-01 00:00:01.420742	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#3] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
13	2005-01-01 00:00:01.420777	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#4] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
14	2005-01-01 00:00:01.420784	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#5] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
15	2005-01-01 00:00:01.420819	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#6] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
16	2005-01-01 00:00:01.420827	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#7] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
17	2005-01-01 00:00:01.420860	2040::60f1:52e4:af04:72da	2142::2038:1a37:e72f:1885	TCP	86	[TCP Dup ACK 9#8] 49244 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0

8

FORTINET

## IPv6: Reverse Path Forward (RFP)

- RFP support added for IPv6

```
id=13 trace_id=9 func=resolve_ip6_tuple_fast line=2737 msg="vd-root received a packet(proto=58, 2040::47:22272->2060::54:128)
from port1."
id=13 trace_id=9 func=resolve_ip6_tuple_fast line=2737 msg="vd-root received a packet(proto=58, 2040::47:22272->2060::54:128) from port1."
id=13 trace_id=9 func=resolve_ip6_tuple line=2828 msg="allocate a new session-0001d805"
id=13 trace_id=9 func=vf_ip6_route_input line=458 msg="reverse path check failed, drop"
id=13 trace_id=9 func=ip6_session_handle_no_dst line=2853 msg="trace"
```

9

FORTINET

## TCP Reset when session automatically closed

- Some protocols remain open but send no data unless there is a change
  - » Example: RDP
  - » Connection is TCP based but no traffic is sent unless there is something from the client or server to update
  - » Default Session timeout is 3600 seconds (1 hour)
  - » After 1 hour of no activity the FortiGate will close down the session. This could result in the loss of connectivity and no error message on the client or server.

10

FORTINET

## TCP Reset when session automatically closed: policy

- Enabled in CLI per firewall policy

```
config firewall policy
  edit (policy_id)
    set timeout-send-rst enable
  end
```

11

FORTINET

## CoS: What is it?

- Class of Services (COS)
  - » Defined by 802.1p IEEE standard

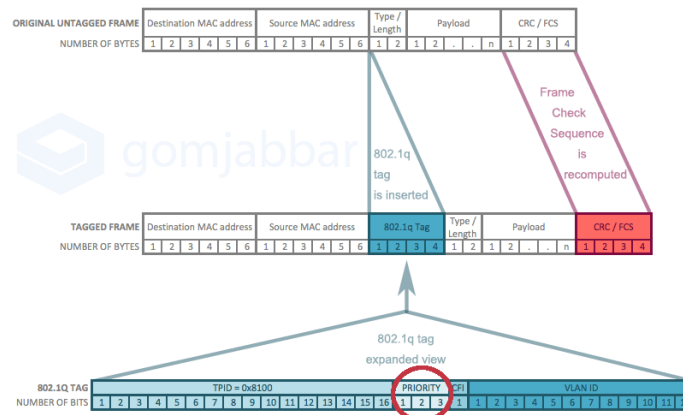
Priority	Acronym	Traffic Types
0 (lowest)	BK	Background
1	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	Video (< 100 ms latency and jitter)
5	VO	Voice (< 10 ms latency and jitter)
6	IC	Internetwork Control
7 (highest)	NC	Network Control

12

FORTINET

## CoS: What does it look like in the packet?

- a 3-bit field within an Ethernet Frame of TCP/IP Layer 2.
- » Part of the 802.1q tag extension for Vlans



13

FORTINET

## CoS: Upgrading

- Previous firmware did not preserve the CoS information in the packets. It was removed.
- 5.2 will now (by default) preserve this information on packets as they pass through



» May result in different network behavior since previously information may have been stripped off.

14


FORTINET

## CoS: Preserve or set?

- Value for CoS in the packets can be preserved or modified on a per IPv4 or IPv6 policy basis
  - » <value> may be : 0,1,2,3,4,5,6,7,255 (255 means passthrough)

```
config firewall [policy|policy6]
    edit (id_number)
        set vlan-cos-fwd (value)
        set vlan-cos-rev (value)
    end
```

15

**FORTINET**

## 5.2 IPsec

© 2014 Fortinet Inc. All rights reserved.  
The information contained herein is subject to change without notice. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

**FORTINET**  
TRAINING SERVICES



## VPN: New Features & Changes

- IPSec Wizard
- Menu Squish
- Automatically route addition
- Multiple interface support
- Authentication against groups
- IPv6 for quickmodes
- IKEv2 cookie notification
- DH Negotiation & Encryption

17

FORTINET

## IPSec: Wizard (GUI only)

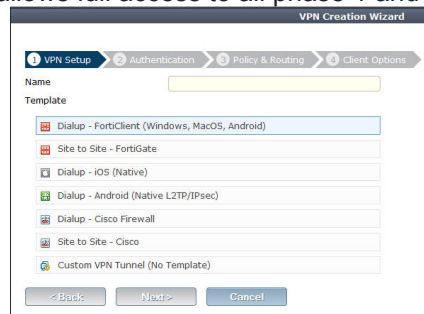
- Creation and Editing of IPSec VPNs is done via the VPN Wizard
- Only Interface based VPNs can be created through the Wizard
  - » Initial Tunnel up policy automatically created
  - » Route(s) automatically added (only Site-to-site)
  - » VPNs created from the CLI do not invoke the GUI Wizard
- Editing Interface VPNs automatically updates routes and policies
- Unable to delete VPN created incorrectly
  - » Policy & Route(s) must be deleted first (object dependency)

18

FORTINET

## IPSec: Wizard Options

- Default templates stored for multiple devices
  - » Automatically set various phase1/2 to device defaults for 3<sup>rd</sup> party vendors
  - » FortiClient, FortiGate, Cisco, iOS, Andriod
  - » 'Custom' allows full access to all phase 1 and 2 settings

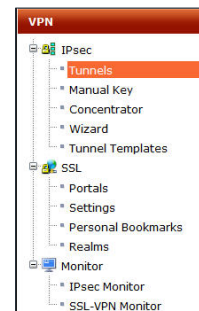


19

FORTINET

## Menu Squish

- 5.0 saw the start of a large push to “Make the FortiGate easier to configure”
- Rather than 2 separate menu options IPSec and SSLVPN are moved into a single menu
  - » Not the only section where this has happened

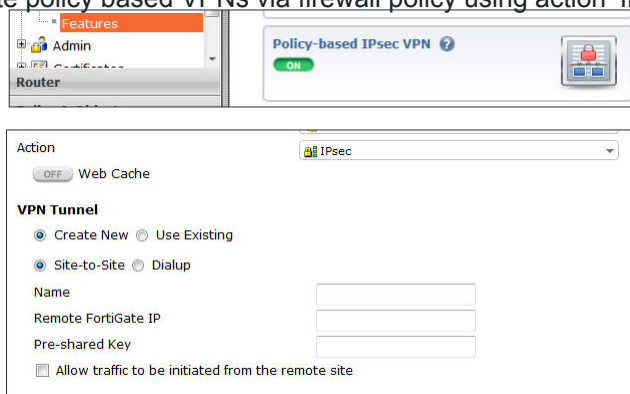


20

FORTINET

## IPSec: Policy VPNs in the GUI

- Creating policy VPNs in GUI requires enabling the option in 'features'
- » Create policy based VPNs via firewall policy using action 'IPSec' (or CLI)



21

FORTINET

## IPSec: Automatic route addition (CLI only)

- Intended for use with BGP over IPSec
- Previously the option was only available in phase 1 when mode-cfg was enabled

» Can be used in phase 1 /phase 2 on any dynamic VPN

```
config vpn ipsec [phase1|phase1-interface|phase2|phase2-interface]
  edit (vpn name)
    set type dynamic
    set add-route enabled           (phase 1 and phase 2)
    set distance [0-255]           (phase 1 only)
    set priority [0 - 4294967295] (phase 1 only)
  end
```

- Automatically adds route to routing table when tunnel is up

22

FORTINET

## IPSec: Multiple interface support

- IKE/IPSec Policies can now be set to include multiple interfaces
  - » Eliminates need to configure duplicate VPN on a separate interface for redundancy
  - » Works for both Policy and interface based IPSec tunnels
  - » Not possible via Wizard

Edit Policy	
Incoming Interface	port1 X ✓ port3 X
Source Address	all ✓
Outgoing Interface	port2 X ✓ port4 X
Destination Address	test ✓
Schedule	always ✓
Service	ALL ✓
Action	IPsec ✓
OFF Web Cache	

23

FORTINET

## Authentication against groups

- Rather than specify the authentication groups in the Phase 1, they can be specified within the VPN firewall policy itself.
- Available for “Dialup” VPNs
  - » XAuth can be changed by editing the VPN after it's been created

XAUTH	
Type	Auto Server
User Group	Inherit Groups from Policy

Edit Policy	
Incoming Interface	Training-Init ✓
Source Address	Training-Init_range ✓
Source User(s)	Guest-group X ✓ guest X SSO_Guest_Users X

24

FORTINET

## IKEv2 cookie notification

When the FortiGate unit detects that the number of half-open IKEv2 SAs is above the threshold value, to preserve CPU and memory resources, the IPSec VPN dialup server requires all future SA\_INIT requests to include a valid cookie notification payload that the server sends back.

RFC 5996, Section 2.6

- Exact value is hard coded (not configurable) and based on the model.
  - » Small models 1000
  - » Larger models 10,000+

25

**FORTINET**

## IPv6 for quickmodes

- Address objects in phase 2 quickmode selectors now support IPv6 addresses

26

**FORTINET**

## DH Negotiation & Encryption

- Default DH group adjusted to include 14 and 5
- Support added for up to 3 DH groups in both Phase 1 and Phase 2
- ECDSA-256, ECDSA-384, ECDSA-512 auth methods added
  - » RFC 4754

27

**FORTINET**

## 5.2 Client Reputation

© 2014 Fortinet Inc. All rights reserved.

The information contained herein is subject to change without notice. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

**FORTINET**  
TRAINING SERVICES

## VPN: New Features & Changes

- IPSec Wizard
- Menu Squish
- Automatically route addition
- Multiple interface support
- Authentication against groups
- IPv6 for quickmodes
- IKEv2 cookie notification
- DH Negotiation & Encryption

29

FORTINET

## Client Reputation: New Features & Changes

- Summary of Changes over 5.0.x
- Renamed and moved

30

FORTINET

## Client reputation: Summary of Changes over 5.0.x

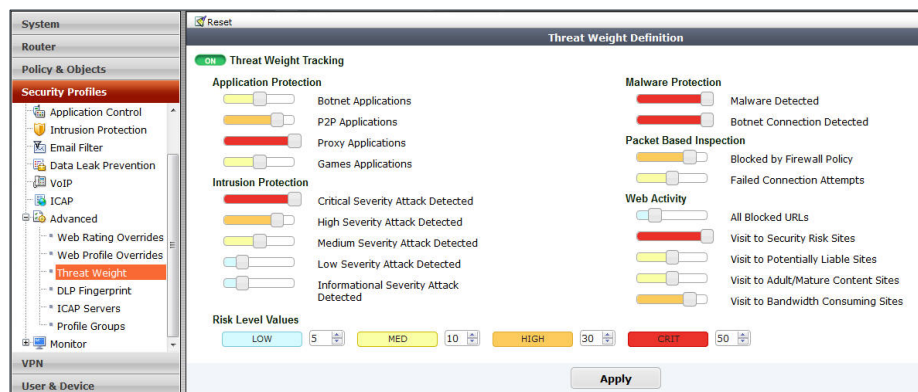
- 5.0.0 any device can enable
  - » Monitoring is done via Client Rep monitor (available on 60+)
  - » Requires SQL logging enabled
- Patch 5 any device still can enable
  - » Now monitored via Threat History Widget
    - Requires SSHD
    - Requires Non-SOHO device

31

FORTINET

## Renamed and Moved

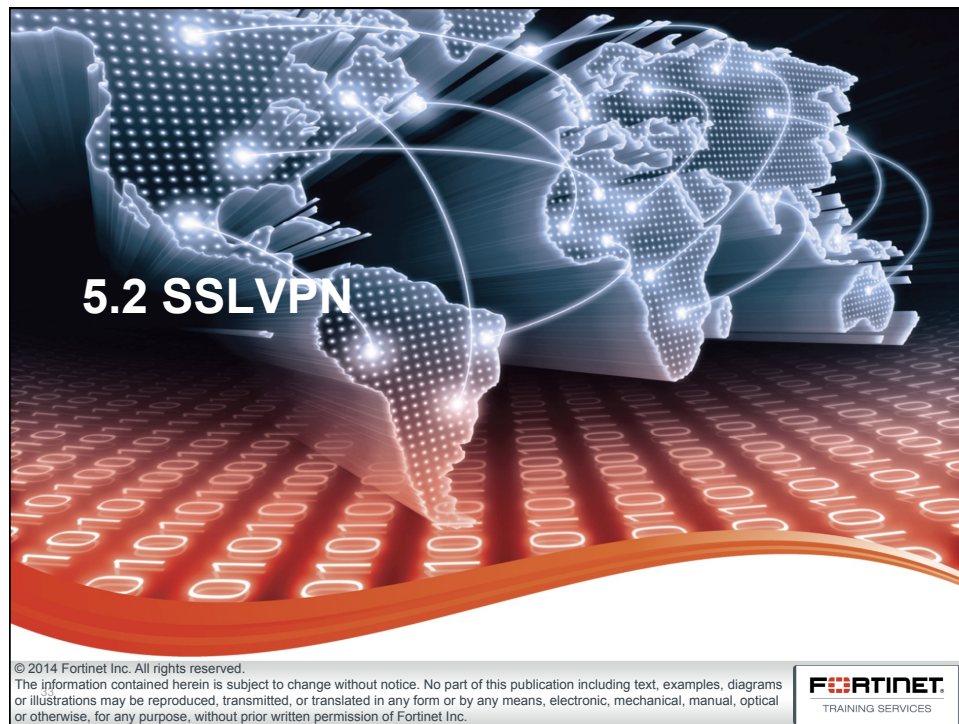
- Renamed to “Threat Weight”
  - » due to link with Threat History widget



32

FORTINET





## SSLVPN: New Features & Changes

- Overall Configuration Change

## Feature Overview – Motivation

- In relation to the Identity policy changes, the motivation behind these SSLVPN improvements come from an NFR

“Customer feedback on VPN config is not good regarding doubled up policies, hence the recommendation to put the session establishment right back in the respective subsystems. Keep using the policy engine for traffic forwarding policy purposes - SSLVPN and interface-mode IPSEC.”

“Elimination of the perceived complexity of the existing engine”

35

FORTINET

## Feature Overview – Remove SSL-VPN Policy Sub-type

- tunnel mode and web mode configurations will be unified
- identity-based configuration will be removed
- policy definition will be consistent with firewall policy in 5.2
- Changes:
  - user can create 1 policy that covers both tunnel & web mode (as enabled), and the SSL daemon will take care of installing the necessary policies to the kernel
  - Services will be used to also control the web portal service options (currently found in SSL Portal Profile)
  - action will be allow/deny
  - user/group will be configured, and also used for authentication
  - Select “ssl.root (sslvpn tunnel interface)” as source
  - Device identification is not an option

36

FORTINET

### Feature Overview – Prompt for conflict of ssl-vpn and admin GUI

- Our default admin HTTPS GUI port is 443. Also, the default SSL-VPN port is 443.
- When both are enabled on the same interface, it will cause a conflict.
- The default is that when both are enabled, we should let SSL-VPN take a higher priority, this means when user connect to 443 port that has both admin GUI and SSL-VPN, we only show SSL-VPN GUI.
- We should have some a warning prompt in FOS to alert user of this conflict.

37

FORTINET

### Feature Overview – SSL VPN GUI 'Settings' Improvements

- The current VPN > SSL > Settings page presents a big list of random options which are not very easy to understand, especially for low end users:
  - » Restricting Source IP is more like optional and not the most important setting
  - » "Port Precedence" is very confusing what it's related to
  - » Assigning the IP Pool in this place only is useful for multiple portal scenarios that want to use overlapping IP range (rare in low end)
  - » The items are not organized in an intuitive way
- New GUI consolidates these settings

38

FORTINET

## Basic Setup, Step 1 – User/User Groups

### 1. Define the user/user groups to be allowed by the SSLVPN

The screenshot shows two screenshots of the FortiGate web interface. The top screenshot shows the 'User' configuration page with a table of users. The bottom screenshot shows the 'User Groups' configuration page with a table of user groups.

User Name	Type	Two-factor Authentication	Ref.
guest	LOCAL	<input type="checkbox"/>	1
sslkeith	LOCAL	<input type="checkbox"/>	1

Group Name	Group Type	Members	Ref.
Guest-group (1 Members)	Firewall	guest	0
SSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)		0
ssl1 (1 Members)	Firewall	sslkeith	0

39

FORTINET

## Basic Setup, Step 2 – VPN->SSL->Portals configuration

### 2. Add/Modify Portals adjust the behaviour of Web and Tunnel mode SSLVPN portals that users are presented with after login

The screenshot shows the 'SSL Portals' configuration page in the FortiGate web interface. It displays a table of portals with columns for Name, Tunnel Mode, Web Mode, and Ref.

Name	Tunnel Mode	Web Mode	Ref.
full-access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1
tunnel-access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
web-access	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1

40

FORTINET

## Basic Setup, Step 3 – VPN->SSL->Settings

### 3. Configure the SSLVPN interface settings under VPN->SSL->Settings

**SSL-VPN Settings**

No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)  This is generally your external interface (i.e. wan1)

Listen on Port  Admin HTTPS Conflict

Restrict Access ☐ Allow access from any host ☒ Limit access to specific hosts

Hosts

Idle Logout ☐ Logout users when inactive for specified period ☐ Never logout inactive users

Inactivity For  (Seconds)

Server Certificate

Require Client Certificate ☐

**Tunnel Mode Client Settings**

Once connected in tunnel mode, clients will receive these settings.

Address Range ☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges

DNS Server ☒ Same as client system DNS ☐ Specify

Specify VPN Servers ☐

Allow Endpoint Registration ☐

**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Users/Groups	Portal
All Other Users/Groups	Full-access

While the port conflict doesn't pose any problems initially, it will take over your admin session if this is not changed after the rest of the config is defined

41

FORTINET

## Basic Setup, Step 3 – Limiting Access

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)  This is generally your external interface (i.e. wan1)

Listen on Port  Web mode access will be listening at https://172.17.97.162:8443

Restrict Access ☐ Allow access from any host ☒ Limit access to specific hosts

Hosts

- “Listen on Interface(s)” allows user to specify which interface(s) to accept client connections from. This replaces the need to configure a *wan->internal* policy for portal access in 5.0
- Further restrictions can be applied with the “Restrict Access” Hosts list

42

FORTINET

## Basic Setup, Step 3 – Negated addresses

- a source-address-negate option in CLI enables users to apply negation to the list of hosts, thereby setting a list of “Restrict Access” hosts to disallow

```
FGT60C # config vpn ssl settings
FGT60C (settings) # set ?
...
source-interface      SSL VPN source interface of incoming traffic.
source-address        Source address of incoming traffic.
source-address-negate Enable/disable negated source address match.
source-address6       IPv6 source address of incoming traffic.
source-address6-negate Enable/disable negated source IPv6 address match.
...
FGT60C (settings) # set source-address-negate enable
FGT60C (settings) # set source-address PC1
```

43

FORTINET

## Basic Setup, Step 3 – Tunnel mode

### Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range ☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges

DNS Server ☒ Same as client system DNS ☐ Specify

Specify WINS Servers ☐

Allow Endpoint Registration ☐

- The Tunnel Mode Settings are defaults that apply to all tunnel mode configs
- The Address Range applies to all tunnels that have not explicitly defined a range under the SSL->Portals Profiles
- If the Automatically assign addresses option is chosen, the default SSLVPN address range `SSLVPN_TUNNEL_ADDR1` is used

Address Range ☒ Automatically assign addresses ☐ Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

44

FORTINET

## Basic Setup, Step 3 – Default Portal & portal options

**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Users/Groups	Portal
ssl1	full-access
All Other Users/Groups	web-access

- Instead of configuring user groups & portal mapping under the Identity-based policy (like 5.0), this is done under the SSL-VPN Settings page
- “default-portal” allows users/groups not defined in the mapping to map to a default portal. Proper firewall policies are still required for access
- Setting a default portal is required

```
FGT60C # config vpn ssl settings
FGT60C (settings) # show
config vpn ssl settings
...
set default-portal "web-access"
config authentication-rule
edit 1
set groups "ssl1"
set portal "full-access"
next
end
end
```

```
FGT60C (settings) # config authentication-rule
FGT60C (authentication-rule) # edit 1
FGT60C (1) # set
source-interface SSL VPN source interface of incoming traffic.
users User name.
groups User groups.
portal SSL VPN portal.
realm SSL VPN realm.
client-cert Enable/disable SSL VPN client certificate restrictive.
cipher SSL VPN cipher strength.
auth SSL VPN authentication method restriction.
```

45

FORTINET

## Basic Setup, Step 3 – Split Tunneling

- The new “Routing Address” option on GUI ensures the addresses in that list are routed through the FortiGate, while Split Tunneling is enabled

Name: full-access

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

Routing Address: 192.168.77.0-Subnet

Source IP Pools: SSLVPN\_TUNNEL\_ADDR1

Client Options: ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

```
config vpn ssl web portal
edit "full-access"
....
set split-tunneling-routing-address "192.168.77.0-Subnet"
....
next
end
```

- Upon connection from a PC, routes to this subnet are directed to the SSLVPN GW

```
C:\Users\keithl>route print 192.168.77.0
```

```
IPv4 Route Table
=====
Active Routes:
Network Destination  Netmask  Gateway  Interface  Metric
192.168.77.0  255.255.255.0  10.212.134.201  10.212.134.200  20
=====
```

46

FORTINET

## Basic Setup, Step 4 – Firewall Policy configurations

### 4. Create the appropriate firewall policies to authenticate users and allow tunnel mode access

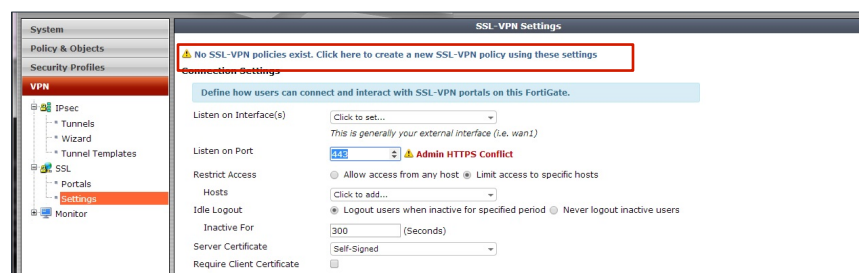
- » In 5.0, a *wan->internal* sslvpn identity based policy with an action of SSLVPN was needed to allow both web and tunnel mode traffic to authenticate and pass through
- » Respective *ssl.root->internal* policies were created automatically per “**auto-tunnel-policy enable**” option
- » In 5.2, the *ssl.root->internal* policy with an action of accept is needed for successful authentication and allowing traffic to pass through into the Lan
- » *ssl.root->WAN* requires if traffic will enter an SSLVPN tunnel from the LAN

47

FORTINET

## Basic Setup, Step 4 – Firewall Policy configurations

- Before a *ssl.root->internal* firewall policy is created, users can neither access web mode nor tunnel mode
- Message on the VPN->SSL->Settings page warns of this



48

FORTINET



## Basic Setup, Step 4 – Firewall Policy configurations

To allow both web mode and tunnel mode access, only 1 firewall policy is required

**Incoming Interface:** ssl.<vdom>

**Source Address:** specify the address range provided for tunnel mode access. This field is meaningless for web mode

**Source User(s):** specify the user group(s) defined in the auth/profile mapping under the VPN->SSL->Settings page

**Outgoing Interface:** specify the network to allow access for

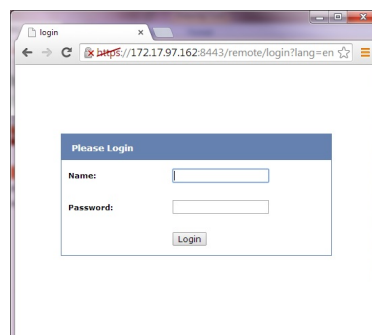
**Destination Address:** specify only the network that is being allowed

49

FORTINET

## Basic Setup, Step 4 – Firewall Policy configurations

- Once the policy is created, you will notice 2 things:
  - » This opens up access to the web portal
  - » The Source access is defined by the “Restrict Access” hosts list



50

FORTINET

## Upgrade – A Basic scenario



ID	Seq.#	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS	Email Filter	DLP	Log	Count
internal - wan1 (1 - 1)														
1	1	all	always	ALL	Accept									5,385 Packets / 689.60 KB
ssl.root (sslvpn tunnel interface) - wan1 (2 - 2)														
8	3	all	always	ALL	Accept									0 Packets / 0 B
wan1 - internal (3 - 3)														
3	2	local			SSL-VPN									85 Packets / 39.30 KB
2.1														
			always	ALL	Accept									
2.2														
			always	ALL	Accept									
Implicit (4 - 4)														
4		all	always	ALL	Deny									

ID	Seq.#	Destination	Schedule	Service	Groups	Action	NAT	AV	Web Filter	Application Control	IPS	Email Filter	DLP	Log	Count
internal - wan1 (1 - 1)															
1	1	all	always	ALL		ACCEPT									4,376 Packets / 687.65 KB
ssl.root (sslvpn tunnel interface) - internal (2 - 3)															
3	2	local	always	ALL	ssl	ACCEPT									0 Packets / 0 B
9	3	local	always	ALL	ssl2	ACCEPT									0 Packets / 0 B
ssl.root (sslvpn tunnel interface) - wan1 (4 - 4)															
8	4	all	always	ALL		ACCEPT									0 Packets / 0 B
Implicit (5 - 5)															
5		all	always	ALL		DENY									

» Note the changes to firewall policies

51

FORTINET

## Upgrade

- » The wan->internal policy has been replaced by a listening interface
- » ssl.root->internal policies replace the ID based policies
- » sslvpn-portal option is moved to SSL->Settings

```
config firewall policy
edit 3
set srcintf "wan1"
set dstintf "internal"
set srcaddr "all"
set dstaddr "local"
set action ssl-vpn
set identity-based enable
config identity-based-policy
edit 1
set schedule "always"
set logtraffic all
set groups "ssl"
set service "ALL"
set sslvpn-portal "full-access"
next
edit 2
set schedule "always"
set groups "ssl2"
set service "ALL"
set sslvpn-portal "web-access"
next
end
next
```



```
config firewall policy
edit 3
set srcintf "ssl.root"
set dstintf "internal"
set srcaddr "all"
set dstaddr "local"
set action accept
set schedule "always"
set service "ALL"
set logtraffic all
set groups "ssl"
set nat enable
next
edit 9
set srcintf "ssl.root"
set dstintf "internal"
set srcaddr "all"
set dstaddr "local"
set action accept
set schedule "always"
set service "ALL"
set groups "ssl2"
set nat enable
next
```

52

FORTINET



### Authentication: New Features

- New Authentication server type
- Maximum number of Guest users
- SSO\_guest\_user behavior

## New Authentication server type: POP3/POP3S

- Authentication can now be done through an external POP3/POP3S server
  - » Users would authentication using their email address and email password

55

FORTINET

## Maximum number of Guest users

- Limit the maximum number of **guest user** per **guest user portal**

The screenshot shows the FortiWiFi 60C Beta 2 interface. The left sidebar has 'User & Device' selected, with 'User' expanded. The 'New User Group' configuration page is displayed. Under 'Guest Management', the 'Maximum Accounts' field is set to 30, highlighted with a red box. A blue callout bubble points to this field, stating 'Maximum guest account allowed is 30'.

Below the configuration page is the 'Guest User Management' table. It shows a list of users with columns for 'User ID' and 'Expires'. An error message is displayed over the table: 'Error: Maximum number of entries has been reached.' A blue callout bubble points to this error, stating 'Guest portal admin will get an error when he attempted to created more than the configured maximum account'.

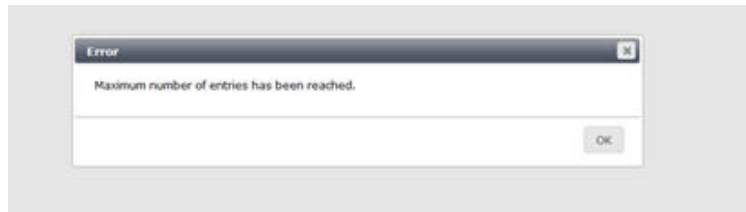
User ID	Expires
DUVUGAdf	st login
CSq434p	st login
m7dVc2Ep	st login
PGq2UwX	st login
3u2hU5	st login
eq2D6W	4 Hours after first login
S3vraMbf	4 Hours after first login

56

FORTINET

## Maximum number of Guest users: Administration

- If an administrator or Guest User Administrator attempts to create more guest accounts than maximum allowed for that group, they will get an error message.



57

FORTINET

## SSO\_guest\_user group behavior

- If only passive authentication is enabled, and the user is not part of any other group, then they will be considered part of SSO\_guest\_user
- If passive and active authentication is used and the user cannot be determined passively, then active authentication will determine the user.
  - » Group membership will be based on the active username

58

FORTINET



## SNMP: New Features & Changes

- USB Modem
- Per VDOM CPU & Memory
- AES256 support

## USB Modem: Logs & Traps on detection and removal

- SNMP Traps and Log messages will be create when a USB modem is plugged in as well as when it is removed
  - » Details include vendor id and product id for proper device identification

61

FORTINET

## Per VDOM CPU & Memory levels: Estimated

Create New Edit Virtual Domain Delete Switch Management [ root ]						
Name	Operation Mode	Enable	CPU	Memory	Interfaces	
root	NAT	✓	0%	21%	dmz	internal
					mesh.root (SSID: fortinet.mes...)	modem
					ssl.root (sslvpn tunnel interfac...)	wan1
					wan2	wifi (SSID: MooMoo416)
vdom1	NAT	✓	0%	0%	ssl.vdom1 (SSL VPN interface)	
vdom2	NAT	✓	0%	0%	ssl.vdom2 (SSL VPN interface)	
			Total Usage	Total Usage		
			0%	21%		

LabLocation\_Charlie (global) # diag sys vd stats

vdom2 cpu:0% mem:0%

vdom1 cpu:0% mem:0%

root cpu:0% mem:21%

62

FORTINET

## AES256 Support

- Can be enabled from the CLI

```
config system snmp user
    edit "test"
        set priv-proto aes256
    next
end
```

- No GUI support to set AES256 at this time

- » At the moment most SNMP software does not have the option to use AES256
- » Setting is available if there is a security policy in place that requires it

63

FORTINET

End

64

FORTINET